AES-EPO STUDY PROGRAM

FINAL STUDY REPORT

Volume I

IBM **Federal Systems Division,**
Electronics Systems Center, Owego, New York

AES-EPO STUDY PROGRAM
Final Study Report
Volume I

ORIGINATED: _____AES-EPO Staff_____

CLASSIFICATION AND
CONTENTS APPROVAL: _____

PROJECT OFFICE APPROVAL: _____

IBM NUMBER: _____65-562-011_____

CONTRACT NUMBER: _____NAS 9-4570_____

Prepared for the
MANNED SPACECRAFT CENTER
National Aeronautics and Space Administration
Houston, Texas

IBM Electronics Systems Center, Owego, New York

31 December 1965

FOREWARD

A computer concepts study was conducted at the IBM Electronics Systems Center at Owego, New York, under IBM Contract NAS 9-4570, for the Manned Spacecraft Center, Houston, Texas. The objective of the study was to investigate possible solutions to long term and time critical reliability problems as they affect the Apollo Command Module guidance and control computer in its application to the AES mission. Volume I of this final report presents a summary of the work performed during the study, and Volume II presents detailed technical descriptions of the various investigations.

TABLE OF CONTENTS

LIST OF ILLUSTRATIONS

LIST OF TABLES

1.0 INTRODUCTION

The study described by this report was performed under contract NAS 9-4570 for the Manned Spacecraft Center, National Aeronautics and Space Administration, Houston, Texas. Although a specific mission and a specific computer subsystem were used as models for the study, the individual investigations were conceptual in nature rather than attempts to apply existing equipment or techniques. Each concept was investigated to the level required to provide a satisfactory degree of confidence in the feasibility of applying that concept to the specified mission.

1.1 Scope

The study consisted of an investigation of the application of the Saturn V computer and a redundant version of the Apollo backup data adapter as a means of meeting the reliability and mission requirements of a 90-day Earth Polar Orbit (EPO) Apollo Extension System (AES) mission. Packaging; reliability; fault detection and isolation; inflight maintenance in high humidity, zero gravity environments; optimum sparing level; module and channel switching; and other pertinent items were studied in an attempt to determine the required redesign of the subject computer and data adapter subsystem to enable it to meet the guidance and control functional requirements and reliability apportionment of a typical 90-day AES-EPO mission. Limited fabrication demonstrating an approach to sparing in a high humidity, zero gravity environment was also required.

1.2 Objective

The objective of this study was to investigate possible solutions to long-term and time-critical reliability problems as they affect the Apollo Command Module guidance and control computer and its applications to AES missions. Specifically, the Saturn V Triple Modular Redundant (TMR) computer and a redundant version of the Apollo backup data adapter were investigated as a means of solving the time critical reliability problem. A detailed investigation of inflight maintenance or module and channel switching of the computer and data adapter were investigated as a means of solving the long term reliability problem.

1

1.3 Approach

The Saturn V computer and a redundant version of the Apollo backup data adapter were examined to determine how their packaging, reliability and machine organization could be improved to meet the requirements of extended Apollo missions. Several concepts and alternate techniques were investigated as solutions for each of the "problem areas" uncovered by examination of this basic computer system. A reconfigured subsystem was derived by selecting the best solution for each problem area.

2.0 REQUIREMENTS

The investigation performed under this contract was directed toward making the subject computer and data adapter subsystem capable of meeting AES requirements. The principle inputs were mission profile, reliability apportionment, and Block II Apollo Guidance and Control Computer requirements. To avoid duplication of effort between this study and contract NAS 9-3724 (Apollo Backup Study), a rigorous verification that the AES configuration will meet the Block II Apollo functional requirements was deferred to the backup computer study. Care was taken, however, to assure that the memory capacity of the AES computer was sufficient for the mission and that the computation speed was faster than the Block II Apollo computer.

2.1 Mission Profile

A 90-day earth polar orbit mission profile was considered for evaluating system requirements necessary to meet the apportioned reliability. The profile was divided for the purpose of analysis into four primary phases: launch, polar orbit injection, orbit adjustment, and re-entry. The profile for boost and orbit injection is shown in Figure 1, and the profile for deboost and re-entry is shown in Figure 2.

2

The primary function of the AES computer during boost is to monitor the guidance and control of the Saturn vehicle. Guidance during the entire S-IC stage burn period is in accordance with a predetermined time-tilt program. An iterative guidance mode (path adaptive guidance) is used for the S-II and S-IVB powered flight phases. Cutoff of the S-IC and S-II stages occurs when the fuel is depleted to a predetermined level, while cutoff of the S-IVB occurs when the velocity for orbital injection is attained. The functions which must be monitored and the parameters which must be computed by the AES subsystem during boost include:

1) Navigation monitoring -- determine velocity vector, perform coordinate transfer, calculate present position, project gravity vector, generate a gyro drift correction, and determine vehicle attitude;

Coast, Transpose, and Dock

200-nmi Polar Orbit

S-IVB Shutdown
t = 640 sec

SM Light
t = 66 min
Burntime 140 sec

S-II Burnout
t = 543 sec

100-nmi
Parking
Orbit

S-IVB
Relight
Burntime 392 sec

LES Jettison
t = 174 sec

S-IC Burnout
t = 150 sec

Saturn V Launch
t = 0
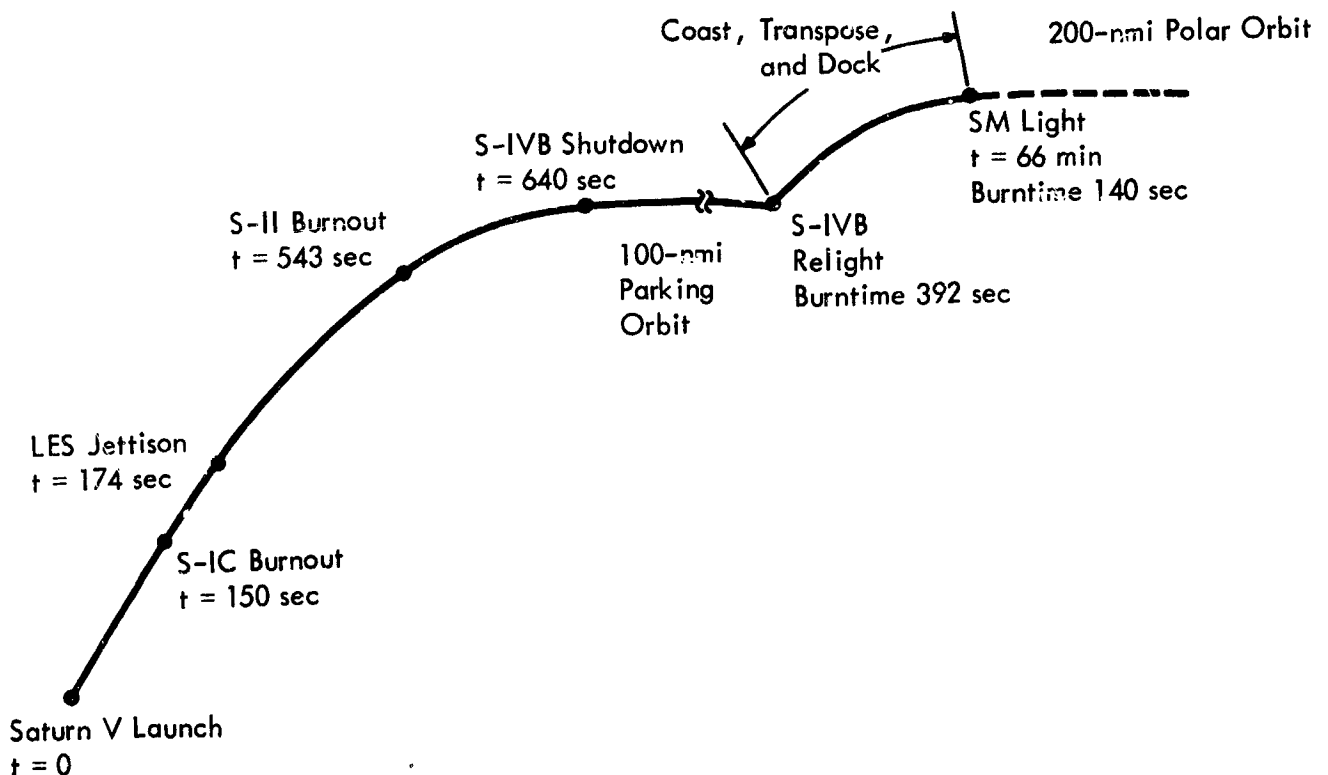
Figure 1. Earth Polar Orbit Mission Profile (with Laboratory)

3

2) Guidance monitoring — compute steering commands, required velocity, engine cutoff times;

3) Control monitoring — engine ignition, engine cutoff, ullage rocket fire, stage jettison;

4) Telemetry transmission of monitored data.

The time periods for the three phases of boost are:

1) S-IC burn — 0.042 hours,

2) S-II burn — 0.110 hours,

3) S-IV3 burn — 0.027 hours,

4) Total (from SOW) — 0.200 hours

200-nmi Orbit   Separate From Laboratory   SM Light Burntime 18 sec

t = 14 min   CM/SM Separation

h = 400,000 ft

t = 6 to 13 min

h = 40,000 ft Parachute Deployment
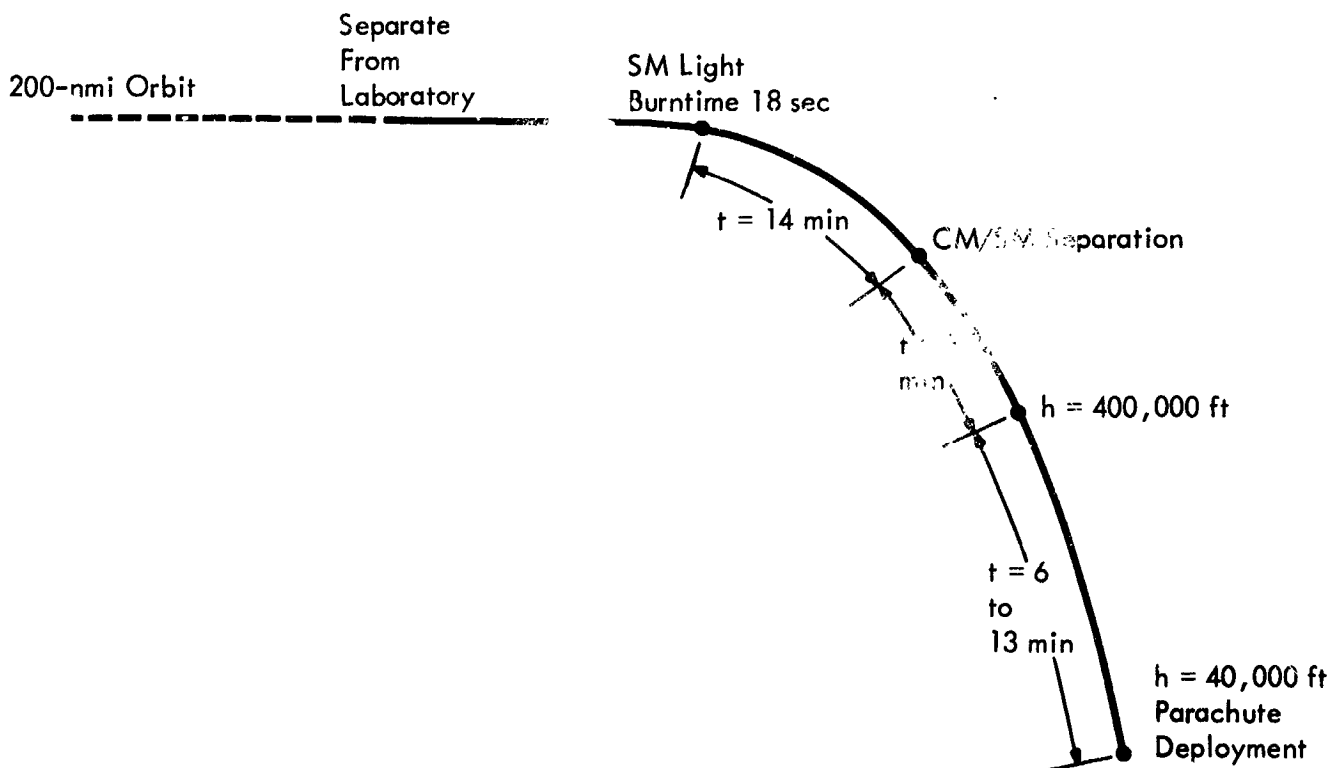
Figure 2. Deboost and Re-entry from Earth Orbit

The primary function of the AES computer during orbit injection (transfer from 100-mile parking orbit to 200-mile EPO) is also to monitor the guidance and control of the vehicle. The AES computer must be capable of providing backup guidance and control with an injection accuracy of 10 nautical miles (one sigma). The time periods for orbital injection and docking are:

1) S-IVB burn — 0.110 hours,

2) SM burn — 0.040 hours.

The AES computer subsystem is required to control vehicle attitude during orbital operations. The required attitude deadband is ±0.50 degrees (all axes) and the allowable drift rates are ±0.02 degrees per second (about zero for two axes and about the orbital rate for the third axis). Powered phases for orbit maintenance are not considered critical for the purposes of this study.

Guidance and control of the command module (CM) and service module (SM) are required of the AES computer subsystem during reentry. This function was examined in detail under contract NAS 9-3724 (the Apollo Backup Study) and the results were factored into Task C (machine organization tradeoffs). The event sequence for reentry from the contract statement of work is:

Time (min)	Event
0	Start re-entry preparations
55.0	Service module ignition
55.3	Service module shutdown
69.0	CM/SM separation
77.0	h = 400, 000 feet
83-90	Parachute deployment (h = 40, 000 feet).

2.2 Environmental Conditions

The environmental requirements for Apollo as defined in specification ND 1002037 were considered valid for AES missions.

The effects of severe environmental conditions occurring during portions of the mission were taken into account in the reliability calculations by applying severity factors to the estimated failure rates (or operating times). Table 1 shows the basic environmental conditions to which the equipment was assumed to be subjected during the various phases of the mission profile.

TABLE 1 — AES 90-Day EPO Environmental Conditions

	Prelaunch	Launch	Orbit	Re-entry
Vibration	None	10-62 cps 0.0025-0.015 g^2/cps 62-380 cps 0.015 g^2/cps 380-2000 cps 0.015-0.003 g^2/cps	Negligible	Negligible
Acceleration	None	6 g	None	10 g
Temperature	20°F to 140°F	20°F to 140°F	20°F to 100°F	20°F to 140°F
Shock	None	20 g	None	(Earth landing) 78 g
Climatic	100% Oxygen 100% RH	100% Oxygen 100% RH	100% Oxygen 100% RH	100% Oxygen 100% RH

The noncritical phases of the mission occur during orbit and are used as the baseline reference for the environmental stresses with a severity factor of unity. The critical phases occur during powered flight and include launch, polar orbit injection, orbit adjustment, and re-entry.

The launch phase is composed of three subphases with varying environmental stresses as shown in Table 2. Launch is initiated by the Saturn-IC booster, which causes the greatest stress to the equipment — 75 times that imposed by orbital environmental conditions. This subphase is followed by the Saturn-II stage burn which imposes 50 times the baseline stress, which is in turn followed by the Saturn-IVB phase with a 35 times stress factor.

TABLE 2 — Launch Stress Factors

Subphase	Time (T) (hrs)	K Factor	$T \times K$
Saturn-IC	0.042	75	3.15
Saturn-II	0.110	50	5.50
Saturn-IVB	0.027	35	0.945
Total	0.179		9.595
Launch K Factor = 9.595/0.179 = 54			

The effective time for each launch subphase is calculated in Table 2 by multiplying the actual time that each subphase exists by the corresponding stress factor. The effective stress factor for the entire launch phase is then calculated by dividing the sum of the effective time periods by the sum of the actual time periods.

During polar orbit injection, thrust is applied to the vehicle by reignition of the Saturn-IVB stage. The stress factor of 35 is applied for the 0.11 hours of burn time. Thrust for orbit adjustment is provided by the service module engine after jettison of the Saturn-IVB stage, and a factor of 25 is applied for 0.04 hours.

The 1.5 hours of critical mission phase designated as re-entry actually includes the time in orbit required to prepare for the re-entry maneuver. It is assumed that the re-entry maneuver will take a maximum of 35 minutes so the orbital factor of 1.0 will be applied for 55 minutes of the 1.5 hours. The re-entry maneuver also consists of two subphases, deboost and re-entry. Deboost is accomplished by reignition of the service module engine. Re-entry stresses are imposed by the acceleration and aerodynamic forces caused by the spacecraft entering the earth's atmosphere. A composite re-entry factor is developed in Table 3 which summarizes the severity factors for each critical mission phase.

TABLE 3 — <u>Re-entry Stress Factors</u>

Subphase	Time	K Factor	T × K
Re-entry Prep.	0.92	1.0	0.92
Deboost	0.005	25.0	5.80
Re-entry	0.58	10.0	0.125
Total	1.505		6.845
Re-entry K Factor = 6.845/1.505 = 4.5			

The resulting stress factors for each of the critical phases are summarized in Table 4 and the corresponding effective time periods calculated by multiplying each severity factor by the actual time during which it is imposed. The "most critical phase" was found to be launch, since it produced the largest effective time of 10.8 hours. Launch was therefore chosen as the phase upon which the computed short term reliabilities were based in the study.

TABLE 4 — <u>Mission Severity Factors</u>

Phase	Operating Time (Hours)	Severity Factor	T × K
Launch	0.20	54.0	10.80
Polar Orbit Injection	0.11	35.0	3.85
Orbit Adjustment	0.04	25.0	1.00
Re-entry	1.50	4.5	6.75

2.3 Reliability

Reliability calculations were made on the basis of the mission profile described in Section 2.1. All channels of the computer and data adapter were required to be operative prior to any critical mission phase, since repair was not allowed during these periods. Repair was allowed, however, during noncritical mission phases.

Reliability calculations were based on duty cycles of 25, 50, and 100 percent of the noncritical phase time combined with the 1.85 hours of the critical phase time. Reliability was calculated on the basis of both a zero failure rate as well as a non-zero failure rate for component electrical off-time. The system required to meet the apportioned reliability was the system based on zero failure rate for off-time.

The apportioned computer-data adapter reliability was specified as 0.9994 for the mission and 0.999999 for the critical phases. A reliability of unity was assumed for the Apollo display and keyboard.

Detailed failure rate data was compiled from an extensive IBM program for collecting and analyzing component part failure data. In addition to observed test and operational data, the failure rates for this study were based on analysis of selected failed parts which related the causes of the failure to basic failure mechanisms peculiar to the part type. From this information, failure rates of parts on which little data was available were formulated by reduction of the part into its basic failure mechanisms. The resulting failure rates are shown in Table 5.

TABLE 5 — Component Failure Rates

Component Part Type	% E. S.	λOp	λ Non-op
Transistors			
Leadless	≤ 10	0.012	0.0023
Leadless, Matched Pair	≤ 10	0.030	0.0048
Silicon, Planar, In Stitched Welded	≤ 10	0.011	0.001
Can	≤ 50	0.017	0.001
Silicon, Planar, Matched Pair, In	≤ 10	0.028	0.002
Stitched Welded Can	≤ 50	0.042	0.002
Silicon, Alloy, Power	≤ 50	0.080	0.0036

TABLE 5 — Component Failure Rates (cont)

Component Part Type	% E. S.	Op	Non-op
Diodes			
Dual, Leadless, Half Used	≤ 10	0.007	0.0016
Dual, Leadless, Both Halves Used	≤ 10	0.006/half	0.0012
Zener, Discrete	≤ 50	0.030	0.002
Silicon, Planar, Micro	≤ 10	0.003	0.0006
Silicon, Planar, Rectifier	≤ 50	0.050	0.0015
Resistors			
Cermet (ULD Type)	≤ 30	0.008	0.001
Metal Film, Precision	≤ 30	0.010	0.0015
Molded, Carbon Comp., Nonhermetically Sealed	≤ 30	0.003	0.0006
Variable, Trimmer	≤ 10	0.080	0.015
Temperature Sensing, Memory		0.010	0.010
Capacitors			
Glass	≤ 10	0.001	0.0004
Ceramic	≤ 30	0.010	0.0005
Tantalum, Solid Section	≤ 50	0.030	0.0014
Connections			
Unit or Page Connector Body		0.003	0.003
Active Connector Pins, Per Pair		0.001	0.0005
Flow Solder		0.001	0.00028
Hand Solder, Memory Frame		0.0005	0.0002
Solder Fillet (ULD)		0.001	0.001
Hand Solder, Memory Address Wire		0.0002	0.0002
Sense or Inhibit Wire		0.00028	0.00028
Splice		0.00036	0.00036
Chip-to-Conductor, Pattern/Ball		0.0005	0.0005

10

TABLE 5 — Component Failure Rates (cont)

Component Part Type	% E. S.	Op	Non-op
Miscellaneous			
Core, Toroidal, T-38		0. 0001	0. 0001
Cable, Flexible, Tape, Per Length		0. 0006	0. 0006
Choke, Filter, Power	≤ 50	0. 12	0. 002
Choke, R. F.		0. 10	0. 002
Crystal, Oscillator		0. 50	0. 003
Delay Line, Glass		0. 30	0. 0025
P. C. Strip, Memory		0. 0001	0. 0001
MIB (1 page side)		0. 553	0. 553
MIB (back panel)		3. 762	3. 762
Transformer, Signal	≤ 50	0. 43	0. 004
Transformer, Power	≤ 50	0. 70	0. 004
Wire, Memory, Per Wire		0. 0001	0. 0001
Transformer, Pulse		0. 100	0. 004
"S Clip", Including Joint-to- Land Pattern		0. 0005	0. 0005
Wrap-Around Land, ULD		0. 0004	0. 0004
ULD Conductor Pattern		0. 0001	0. 0001
Substrates		0. 0001	0. 0001

% E. S.   = Expected percent of electrical stress ratings

λ Op   = Operating failures per 10^{+6} component hours

λ Non-op = Non-operating failures per 10^{+6} component hours

3.0 SUMMARY

The study was divided into four primary areas of investigation: 1) packaging, 2) machine organization, 3) error detection and diagnosis, and 4) fabrication and test. The packaging study was aimed primarily at deriving packaging techniques applicable to operation and maintenance in the high humidity, zero gravity AES environment. The principal goals of the machine organization study were attainment of the extremely high reliability requirement of the AES critical phases and realization of automatic error detection and diagnosis. Error detection and diagnosis studies using the Saturn V System Simulator provided insight to the mechanisms of error propagation in a digital system and produced the data necessary for the machine organization effort. The fabrication and test effort included fabrication of a computer/data adapter mockup, fabrication of representative module packages and a special environmental chamber in which to test them, exploratory tests to determine a satisfactory connector-sealing technique, and evaluation tests of the representative modules.

In general, all phases of the study were successful. A packaging approach was derived which is suitable for operation and maintenance in the adverse AES environment. The reliability requirement of 0.999999 for the critical phases of the AES mission was met by the TMR machine organization which evolved during the study. The reliability requirement of 0.9994 for the 90-day mission was met either by sparing or by automatic repartitioning of the computer system in flight. Automatic error detection was proved by simulation to be feasible with an efficiency of better than 99 percent without interrupting normal machine operation (without special test programs or routines). Automatic fault isolation to a replaceable module level was achieved by built-in circuits. A logic circuit was designed which not only provides the voting, error detection, and fault isolation functions, but automatically switches out the failed component.

No extensive tradeoffs were required or performed during the study. For example, no other forms of redundancy other than triple modular redundancy or variations such as quad redundancy were considered. Similarly, no tradeoffs were made between built-in test circuitry and test programming. As a result, the selected configuration probably is not optimum for the application although it does meet all the requirements specified by NASA-MSC or otherwise known to IBM.

The extremely high reliabilities specified for the AES-EPO mission are reasonable in that they can be met by conventional TMR organization, simple packaging techniques, and existing diagnostic methods. Further investigations would be required to determine whether the automatic repair techniques developed during the study would be worth the cost of the additional equipment complexity when compared to manual module replacement.

3.1 Packaging

Several approaches were investigated for packaging the computer and data adapter for operation and maintenance in the high humidity, zero gravity AES environment. A decision was made early in the study to package the computer and data adapter in a single unit in order to simplify the interconnection problems. Although this decision affects the overall form factor and size of the computer system, it does not affect the relative merits of the various approaches considered or the conclusions of the packaging studies.

The first approach was the conventional packaging technique for aerospace computers in which the computer system is sealed as a unit. Upon removing the unit cover to replace a failed module, the entire interior of the unit is exposed to the spacecraft environment. When the cover is replaced after repair, the free moisture and contaminants trapped in the unit must be purged and the unit repressurized to somewhat greater than cabin pressure with dry gas.

In the second and third approaches an attempt was made to limit the degree of exposure during a maintenance action by sealing various portions of the computer independently. Since a TMR computer consists of essentially three individual computers, each channel can be sealed individually so that only a third of the computer is exposed each time a repair is attempted. In the Saturn V computer, the casting is designed such that each logic channel is partitioned into effectively five physical cells. If each cell is separately sealed, then a fifteenth or less of the computer is exposed each time a repair is attempted.

In each case the covers would be sealed by means of modified 0-rings and the exposed volume purged and repressurized with dry gas to an overpressure of two or three psi. Gasket-sealed units have been designed at IBM to provide leakage rates as low as 10^{-7} cubic centimeters per second per inch of linear seal length.

Tradeoffs between the three sealing approaches were made on the basis of leakage rates, expected repair intervals, module replaceability, and design complexity. Although each method possessed certain advantages over the other two, the cell-sealing approach was selected primarily because it provided minimum circuit exposure over the 90-day mission and because it provided easiest access to a failed module, but at a cost in size, weight, and probably cost of fabrication.

Closed loop systems were considered but not emphasized in the study. A pressurized system which circulates dehumidified air through the computer and contains filters for chemical contaminants has, at least, history in aircraft applications. The use of freon in a closed loop or even static system offers several advantages including moisture-repellent characteristics.

No matter what packaging approach is selected for application in an adverse environment, the problem of sealing the connectors remains a problem. Although the connectors associated with the pluggable modules are partially protected in any of the approaches described above, the cable connectors which connect the computer system with other systems remain exposed to the spacecraft environment. Study emphasis was therefore given to connector sealing techniques.

Exploratory testing of various sealing techniques indicated that a combination of gasket sealing and silicone gel loading of the connectors appeared to solve the connector sealing problem. The test results were so successful, in fact, that the packaging approach selected for the AES computer system eliminated sealing of the replaceable modular area as shown in Figure 3. Each replaceable module is sealed individually and chassis sealing is limited to unreplaceable items such as back panels and interconnecting wiring.

In the exploratory tests of various connector-sealing techniques, a male and female Saturn V page connector were wired and sealed with epoxy on their rear surfaces as shown in Figure 4. A silicone rubber gasket was glued to the face of the female connector with Dow-Corning A9-4000. The female cap was removed and DC-3 silicone grease packed inside the connector. The pins of the male connector were also saturated with DC-3 silicone grease. Contact measurements (made with 40 contacts connected in series) before and after application of silicone grease indicated that the grease had no measurable effects on the contact resistance between male and female connections. Leakage resistance checks between adjacent pins showed no appreciable change in megger readings even when disconnected and reconnected while immersed in a bath of salt water.
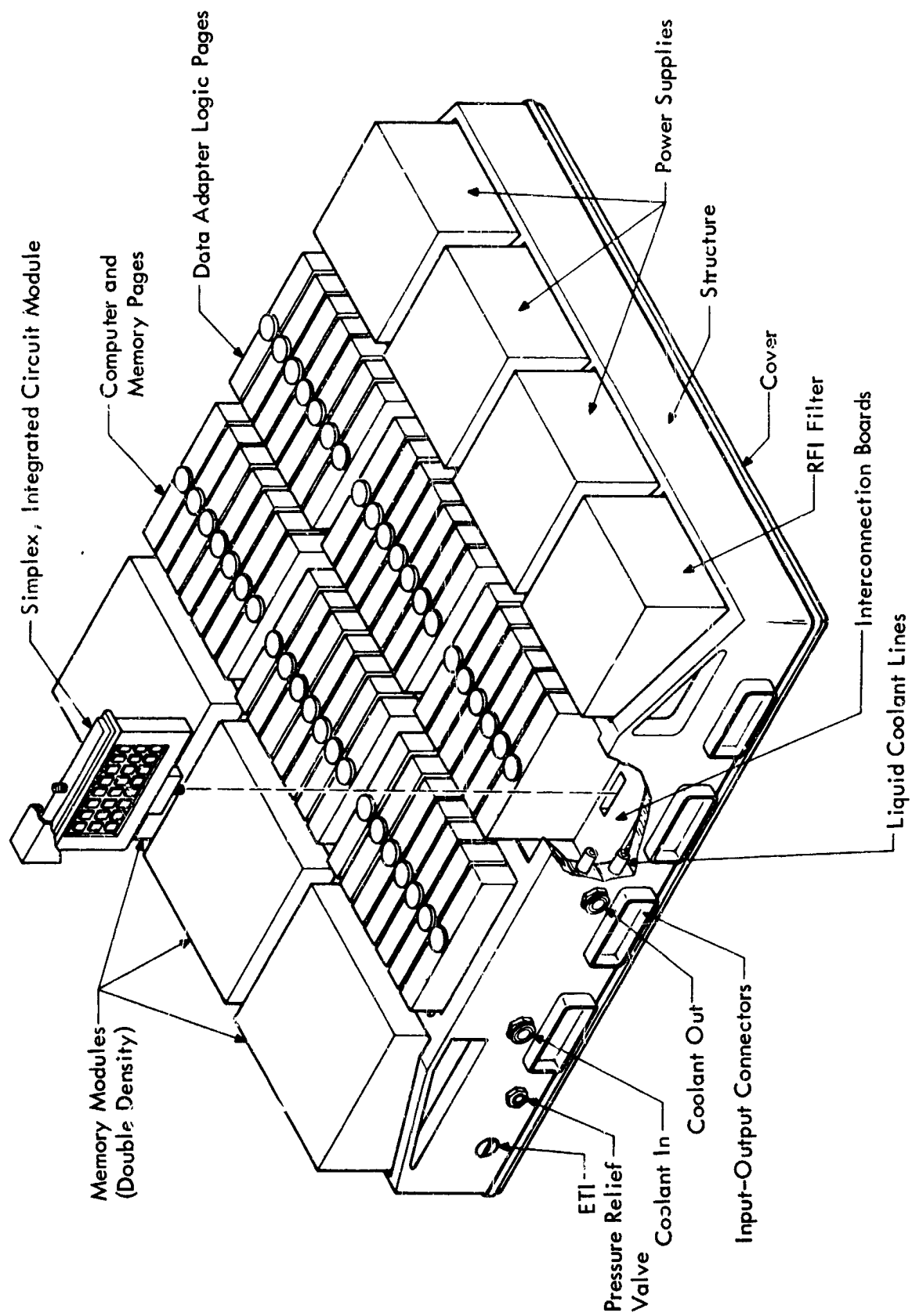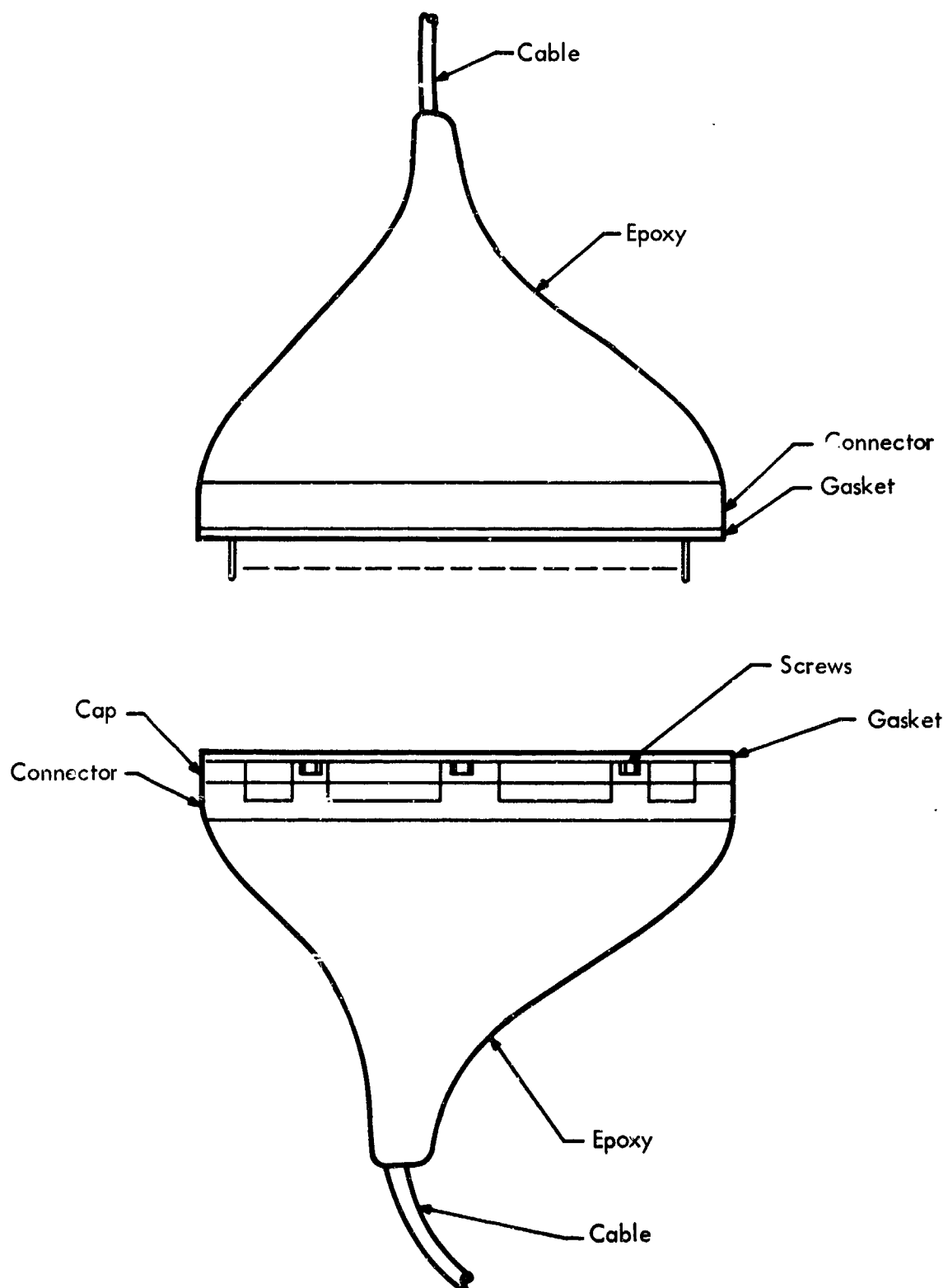
Figure 3. Apollo Computer — AES

15

Figure 4.   Exploratory Test Model

16

Although individual sealing of the replaceable modules and application of the above connector-sealing technique would seem to solve the packaging problem for operation and maintenance in the adverse AES environment, a detailed data analysis of test results on contact materials was performed to assure that the properties of the contact materials would not present a problem in the AES application. This analysis resulted in the recommendation of gold-on-nickle as the contact material, as in the Saturn V connectors, but with the thickness of the gold plating increased from about 50 mils to 200 mils. If the increased plating thickness and stringent quality control methods prove to be inadequate in controlling plating porosity, a technique for welding gold foil on base contact materials has been proven feasible at IBM but not as yet used because of the higher fabrication costs involved. Although the recommended process will result in expensive connectors, their performance in the adverse AES environment seems assured and worth the cost.

3.2   Machine Organization

The Saturn V computer and a redundant version of the Apollo backup data adapter were used as a basic system for the machine organization studies. This basic computer system was analyzed for its reliability, error detection, failure isolation, and performance capabilities and changes to the machine organization made to improve the weak areas uncovered by the analysis.

Simulation of the reliability model for the basic system revealed that neither the time critical nor long term reliabilities were met by the basic system without sparing, as indicated in Table 6. In order to improve system reliability (especially in the critical mission phases), the simplex computer oscillator and the duplex memories and the duplex power supplies were triplicated. A novel oscillator configuration was designed in which three unsynchronized oscillators operate in parallel and are selectively gated into the system according to error detector indications. TMR memories provide a reliability increase by forcing error-causing disagreements from the word level of the duplex configuration to the bit level of TMR voting. Triplex power supplies with overlapping duplex distribution nets were selected as the power system for the reorganized computer system.

Two machine organization areas which were investigated with the purpose of improving system reliability but which were not factored into the reliability computations were grounding and transient protection. The grounding scheme of the Saturn V system was retained in general but revised in detail to reduce interaction of ground currents,

Table 6 — Reliability Estimates (Basic System)

Element	Critical Phase	Mission Reliability				
		100%	Non-op $\lambda > 0$		Non-op $\lambda = 0$	
			50%	25%	50%	25%
Computer	0.999933	0.8879	0.9272	0.9446	0.9647	0.9886
Oscillator	0.999992	0.9984	0.9989	0.9992	0.9992	0.9996
Logic	0.999998	0.9334	0.9580	0.9686	0.9809	0.9947
Memory	0.999942	0.9528	0.9689	0.9760	0.9843	0.9943
Data Adapter	0.999989	0.8096	0.8921	0.9272	0.9429	0.9840
Power Supply	0.999995	0.9980	0.9988	0.9992	0.9992	0.9997
Logic	0.999994	0.8113	0.8932	0.9280	0.9436	0.9843
Computer System	0.999921	0.7189	0.8272	0.8759	0.9096	0.9728

especially at the module interfaces and in the memory modules. Isolated ground planes were provided for the memory modules, since these are the most noise-critical elements in the computer system, but at the cost of transformer-coupled drive circuits and addition of differential amplifiers in the sense lines.

The results of the transient susceptibility tests of the Gemini computer were reviewed to determine their applicability to the AES computer organization. The most transient-sensitive areas of the digital circuits were found to be the memory sense lines and the output lines of the delay line sense amplifiers. Reduction of the susceptibility of the basic computer organization to voltage transients can be achieved in the reorganized system by improving the physical layout of the sense lines, limiting the bandwidth of the sense amplifiers, providing alternate strobing of the TMR memories, and isolating the memory ground planes.

A logic circuit was developed during the study which votes on the triplex logic , detects a disagreement between the three inputs to the voter, isolates the error to one of the three inputs, and turns off the faulty input and one of the two good inputs. If a failure occurs in a module, this logic circuit effectively switches down that module to a simplex operating mode. An automatic TMR/Simplex operating mode was therefore provided for the reorganized system in which one or more modules operate simplex while the rest of the system operates TMR. The reliability estimates for the reorganized computer system

in the TMR/Simplex mode of operation are given in Table 8. Although the TMR/Simplex mode provides reliability improvement over the conventional TMR mode (Table 7), sparing is still required to meet the reliability requirement of 0.9994 for the 90-day mission.

TABLE 7 — Reliability Estimates (Reorganized System)

Element	Critical Phase	Mission Reliability				
		100%	Non-op $\lambda > 0$		Non-op $\lambda = 0$	
			50%	25%	50%	25%
Computer	0.9999994	0.9787	0.9888	0.9930	0.9943	0.9984
Logic	>0.9999999	0.9996	0.9998	0.9999	0.9999	>0.9999
Memory	>0.9999994	0.9791	0.9892	0.9931	0.9944	0.9985
Data Adapter	0.9999997	0.9910	0.9953	0.9969	0.9975	0.9993
Power Supply	0.9999999	0.9999	>0.9999	>0.9999	>0.9999	>0.9999
Logic	0.9999998	0.9911	0.9954	0.9970	0.9976	0.9994
Computer System	0.999999	0.9699	0.9845	0.9901	0.9920	0.9979

TABLE 8 — Reliability Estimates (TMR/Simplex Mode)

Element	Critical Phase	Mission Reliability				
		100%	Non-op $\lambda > 0$		Non-op $\lambda = 0$	
			50%	25%	50%	25%
Computer	0.9999995	0.9817	0.9905	0.9939	0.9951	0.998i
Logic	>0.9999999	0.9998	0.9999	0.9999	>0.9999	>0.9999
Memory	>0.9999995	0.9819	0.9906	0.9940	>0.9951	>0.9987
Data Adapter	0.9999999	0.9955	0.9977	0.9985	0.9988	0.9997
Power Supply	>0.9999999	0.9999	0.9999	>0.9999	>0.9999	>0.9999
Logic	>0.9999999	0.9956	0.9978	>0.9985	>0.9985	>0.9985
Computer System	0.999999	0.9772	0.9882	0.9924	0.9939	0.9984

The mission reliability can be satisfied with the inflight spares complement given in Table 9. Neglecting the critical phase requirements, the long term reliability can also be met by operating the computer in a simplex mode and switching in spares from the two non-operating channels as failures occur in the operating channel.

TABLE 9 — Spares List

Spare Number	Subassembly Name	Delta Reliability	Cumulative Weight (lbs)	System Reliability
11	Input/Output	0.00737480	0.43	0.97749496
4	Memory Module	0.01608645	4.93	0.99358141
11	Input/Output	0.00071146	5.36	0.99429286
4	Memory Module	0.00443837	9.86	0.99873123
1	Arithmetic	0.00012259	10.29	0.99885383
9	Control	0.00012093	10.72	0.99897476
3	Control Timing	0.00011069	11.15	0.99908544
8	Data Flow	0.00009657	11.58	0.99918202
7	Time Counter	0.00009165	12.01	0.99927367
6	Input Counter	0.00008464	12.44	0.99935830
10	Processor	0.00008128	12.87	0.99943958

12.87 pounds of spares required

In the Apollo Backup Study it was found that the Saturn V computer with its ULD (unit logic device) circuit technology did not possess sufficient computational speed to perform the Apollo control function. A separate control processor was added to the Apollo data adapter to handle the control function. A four times speedup in the reorganized AES computer was realized by increasing the oscillator frequency and converting from ULD to monolithic integrated circuit (diode-transistor logic family) technology. The preceding reliability estimates for the reorganized computer system reflect this shift in circuit technology.

The machine organization study included an investigation of the effects of breaking up the computer into various levels by modularization. This portion of the study was limited to the computer (excluded the data adapter) since data was available on several computers including the Saturn V computer.

The increase in circuitry required as the Saturn V computer is partitioned into various numbers of pluggable modules is shown in Figure 5. Modularization was found to have only moderate affect on the
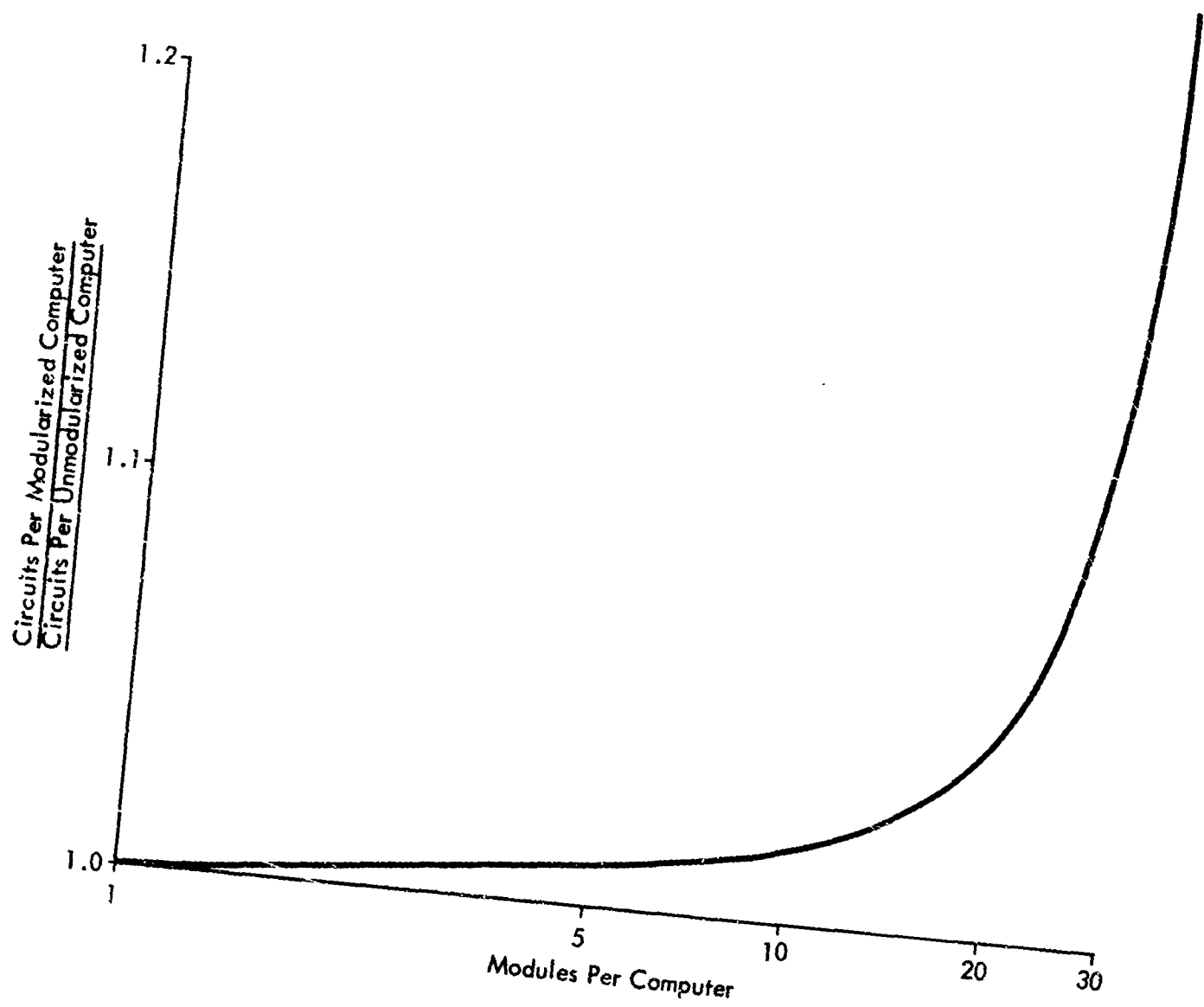
20

Figure 5. Increase in Circuitry with Modularization

21

total amount of circuitry required by the computer organization in the range from an unmodularized unit to about ten modules. As the computer is partitioned into modules greater than ten, however, the required circuitry increases very rapidly (primarily because this lower-level partitioning cuts across functional areas). The Saturn V computer was organized into seven functional areas but partitioned into more than ten pluggable modules per channel. The reorganized AES computer was partitioned into four pluggable modules per channel.

The functional relationship between the total intermodule connections per circuit as the partitioning is carried to lower levels results in a similarly shaped curve with the break point at about ten modules. The same general relationship exists between modularization and the total number of voters required per machine. Although the AES computer was partitioned into four modules primarily to optimize the failure isolation capabilities of the built-in detection circuitry, this modularization level is well within the cost constraints of total circuits, intermodule connections, and total number of voters required.

The data adapter portion of the AES computer system was analyzed in a similar manner resulting in a partitioning of seven pluggable modules per channel. The final partitioning of the computer system is summarized in Table 10. Some of the basic characteristics of the reorganized computer and data adapter are listed in Tables 11 and 12, respectively.

TABLE 10 — Computer System Partitioning

Module	Function	Section
1	Memory and Memory Interface	Computer
2	Arithmetic (Including Mult and Div)	Computer
3	Address Registers	Computer
4	Control and Timing	Computer
5	Output Counter	Adapter
6	Input Counter	Adapter
7	Time Counter	Adapter
8	Data Flow	Adapter
9	Control	Adapter
10	Processor	Adapter
11	Output Drivers	Adapter
12	Power Supply	Power Supply
13	RFI Filter	Power Supply

TABLE 11 — Computer Characteristics

Type	General Purpose, Serial, Fixed Point
Organization	Triple Modular Redundant, Self-reorganizing, Modularized
Speed	40,000 ops/s, 21 Microsecond Add
Word Length	26 Bit Data, 13 Bit Instruction
Memory	Double Density, TMR, 16K Equivalent Instructions
Size	69 Pounds, 1.8 Cubic Feet
Power	102 Watts (Including Power Supply)

TABLE 12 — Data Adapter Characteristics

Item	Function	Description
Inputs	Discrete Pulsed	73 33 (Serial and Incremental)
Outputs	Discrete Variable Pulsed Fixed Pulsed	68 43 (Serial, Incremental, Discrete) 10
Modules	Output Counter	11 (Including Registers and Control), Gyro and Radar Counter Logic
	Input Counter	11 Counters, Multiplexer, Hand Control Logic, Bootstrap Loader
	Time Counter	9 Counters, Pulse Timing
	Data Flow	Data Exchange Register, Logic, Multiplexer
	Control	4 Discrete Output Registers, Address Decode, Controls
	Processor	Load Register, Down Link Register and Control, Interrupt Register
	Input/Output	Simplex Drivers

3.3 Error Detection and Diagnosis

One of the ground rules which was established early in the study was that error detection and diagnosis of the computer system be automatic. An additional ground rule was that the error detection and fault isolation functions be simultaneous with normal system operation rather than interwoven or serial with the operational program. To satisfy these ground rules a built-in test circuit approach was chosen as the primary method for inflight error detection and diagnosis. No check routines (such as reasonableness tests), test programs, or diagnostic programs which would interrupt system operation were considered.

The Saturn V System Simulator was the primary tool for the detection and diagnostic analyses. This simulator consists of a set of IBM 7090 programs which simulate the detail logic behavior of any digital system which can be logically described on a master tape. One important feature of the simulator allows the injection of logic faults into the simulated system to examine the phenomenon of error propagation, and this feature was used to evaluate the error detection and fault locating capabilities of the built-in test circuitry. Simulator flexibility also allowed the effects of various partitioning schemes to be evaluated and thus provided a rapid method for optimally placing voters and error detectors in the system organization.

In the TMR Saturn V computer and data adapter, disagreement detectors provide an output if any of the triplicated modules fail. These detectors consist of a three-way exclusive OR connected to the three channel inputs to each voter circuit. These disagreement detectors and several modified variations provided the basic means for detecting errors in the computer system under study. The outputs of these detectors were "OR'd" together in a logical network to provide the basic means for fault isolation.

The simulator was used to determine optimum placement and timing of the detector in the computer system and to evaluate the error detecting efficiency of the built-in test circuitry. In several hundred failure simulations, over 99 percent of all simulated failures were detected. Simulation also proved that failure isolation to a replaceable module level was attained in the reorganized computer system by the disagreement detector "OR'ing" network.

Module and channel switching, both automatic and manual, were investigated as inflight techniques for improving system reliability and for supporting maintenance activities. Single channel operation of some modules or of the entire system for selected mission phases or operational conditions was considered.

Two new modes of operation were derived: 1) TMR/Simplex and 2) TMR/Switchable Spare. In the TMR/Simplex mode, one or more modules of the system may operate simplex while the remainder of the system operates TMR. One operational simplex module is turned off with every failed simplex module, resulting in an appreciable system reliability increase over the basic TMR mode. An even greater reliability increase is provided (at the cost of additional test and switching circuitry) by the switchable spare mode in which the turned off operational module is made available as a spare for the operating simplex module in the TMR/Simplex mode.

For maximum long-term reliability in noncritical phases of the mission, the system may be operated in the simplex mode with two inoperative channels available as built-in spares. The "multiprocessing" potential of operating the three channels of the TMR system as three independent systems capable of performing independent functions of life-support system processing, experimental system processing, and vehicle control (for example) has been found to be feasible. Further study is required to achieve this potential, however, by developing means for decoupling channels, as well as simply controlling their on-off status.

The voting and switching logic developed during the study has made possible an on-line repair capability for the computer system while operating in the TMR mode. Failed modules may be replaced with spare modules without interrupting normal operation of the system. Similarly, automatic self-repair capability is feasible with the new logic by instrumenting a fourth or spare channel. The new logic will detect a disagreement between the three operating channels, isolate the failure to the specific module and channel, turn off the failed simplex module, and switch in the spare from the inoperative fourth channel.

A primary goal was defined early in the study to automate the error detection and fault isolation functions and thereby minimize crew requirements for inflight maintenance. Training, experience, and test information required by the crew to effect repair were made negligible by the hardware approaches pursued in the study. Man-in-the-loop operations required by the AES instrumentation were limited to reading a bank of indicator lights to determine the location of a failure and to making a manual replacement of the failed module. Test and packaging approaches were directed toward eliminating the need for special test equipment or special tools to effect inflight maintenance. Semiautomatic repair methods in which the astronaut switches in wired-in spare modules or changes operating mode were also investigated, as well as fully automatic repair and mode changing.

3.4 Fabrication and Test

Limited fabrication and test was required in the study to prove the feasibility of inflight maintenance in a high humidity, zero gravity environment.

A nonfunctional mockup was fabricated of the reconfigured computer system illustrating the organizational and packaging concepts selected during the study for AES applications. As shown in the photograph of Figure 6, a departure from the conventional sealed unit designs of aerospace computers was made in favor of individually sealed modules. In this packaging approach the only sealing problems lie with the connectors — both module and cable connectors.

Exploratory tests performed on the Saturn V page connectors resulted in the selection of a gasket-silicone gel sealing technique for the AES connectors. Several connectors were loaded with silicone gr⁻ ˙ se and tested for contact resistance and leakage resistance between adjacent pins. The grease had no measurable effect on contact resistance for all connectors tested. Immersion tests for leakage resistance showed the need for a gasket in addition to the grease to provide a pin-wiping action both on insertion and disconnect of the male half of the connector with the female. With the gasket-grease combination, the connectors were mated and remated while immersed in salt water with no appreciable change in megger readings between adjacent pins.

Nine representative replaceable modules were prepared to illustrate a solution to the problem of packaging and sparing for the adverse AES environment by modifying Saturn V breadboard computer logic pages. The page itself was sealed with a rubber compound (RTV) and the female connector (in the test equipment) which mates with the page was prepared with the gasket-silicone gel combination. A photograph of a modified module and the mating female connector is shown in Figure 7.

A special environmental test chamber was fabricated (Figure 8) to provide simulation of the high humidity, zero gravity AES environment. The water tank on the lower left-hand side of the chamber is equipped with heater, blower, and controls to produce a relative humidity varing between 80 and 100 percent. The temperature within the chamber was maintained in the region of 100°F to 125°F. To simulate the migration effects of free moisture to electrical connectors in zero gravity, a water solution of 0.22-percent sodium chloride and up to 1 percent urea was sprayed on the test modules once each hour for the entire continuous test period of 58 days. An electrical charge was applied to the spray to simulate ionization of free moisture. Rubber gloves sealed to one

wall of the chamber allowed modules to be unmated and remated at intervals during the test period without affecting the chamber environment, thus simulating maintenance activity (module replacement) and perhaps the suited astronaut conditions.
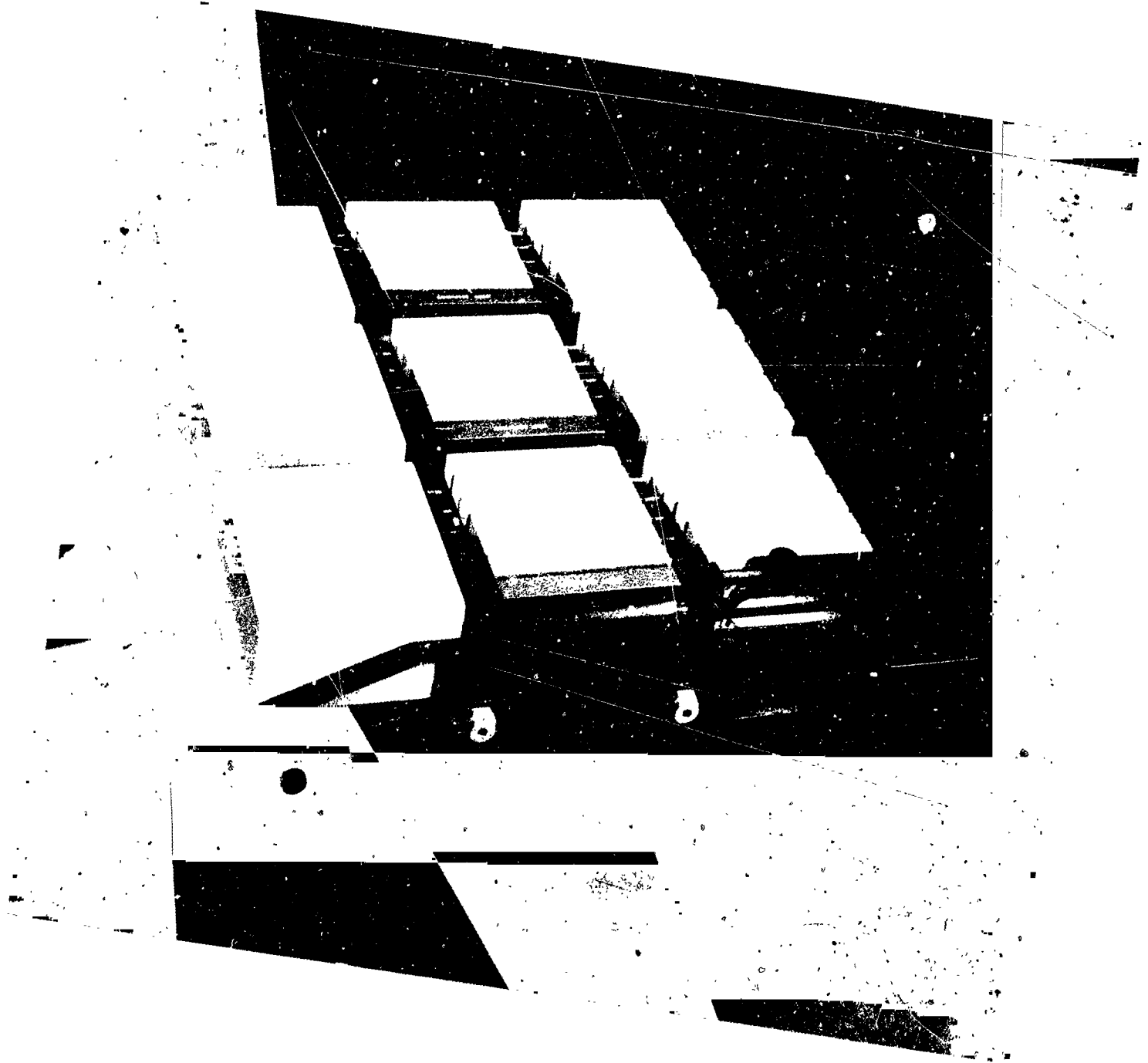

Figure 6. Computer Mockup

Figure 7. Representative Replaceable Module

A Phase II testing program was initiated on 4 October to evaluate the gasket-silicone gel technique for sealing connectors. Although the purpose of Phase II testing was not to evaluate sealing of the module itself (replaceable modules in the AES computer would be hermetically sealed as individual components), the Saturn V pages used to represent AES replaceable modules had to be sealed to prevent logic failures in the high humidity environment while testing the connector sealing technique.

DC voltages were applied to certain pins of each module, and approximately 20 pins were monitored on each module for changes in the resulting static patterns. Very few test points showed any appreciable change in voltage level during the first month of testing although the magnesium-lithium frames of the Saturn V logic pages showed drastic deterioration. Those test points which did exhibit appreciable change (over 5 or 10 millivolts) were found to be located on those pages showing the most frame deterioration indicating that the voltage changes resulted from moisture leakage around the frames (under the RTV seal) rather than at the connector.

28
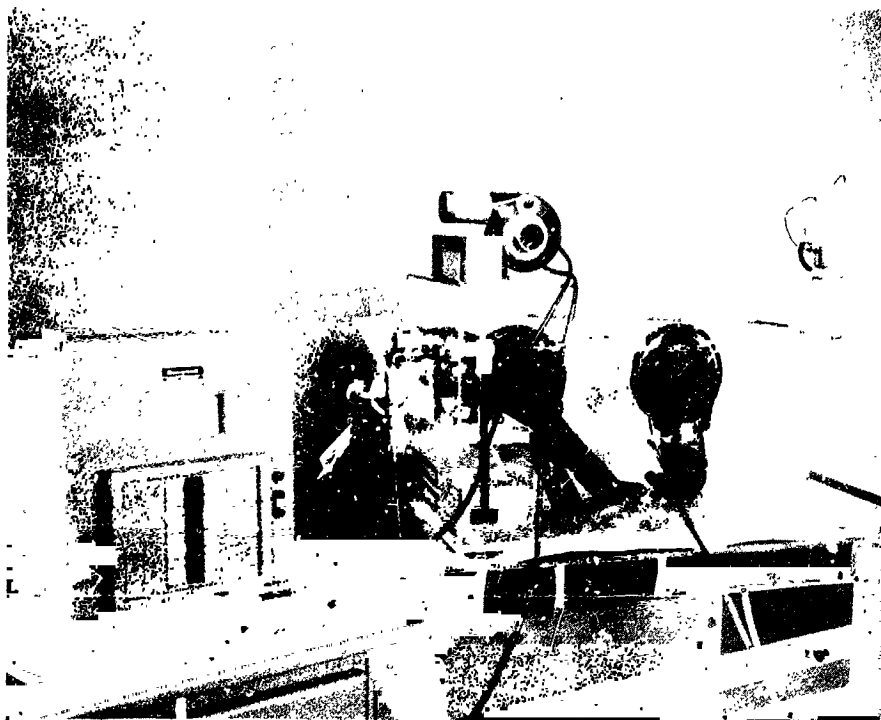
a. Before Test

b. During Test

Figure 8. Environmental Test Chamber

On 7 November the tests were interrupted by a failure of the test chamber. A connection came loose from the water tank causing a flooded condition and drastic changes in the temperature-humidity environment. A rash of voltage changes occurred at this time, especially on those modules exhibiting the most frame deterioration.

It is difficult to define a voltage change as a failure, since the operation of digital systems is on-off in nature. Even the most drastic changes in voltage levels monitored during the test may not cause a logic failure in actual practice. For the purpose of this discussion, however, a logic failure is defined as a voltage change of over 25 millivolts.

Of the nine representative modules, six exhibited no failures until the test chamber failed (a test period of over a month). Two modules survived the flood and exhibited no failures for the entire test period (57 days). One module exhibited one failure, and a second module exhibited two failures after the flood. One of the modules which operated perfectly up to the time of the flood had to be disconnected following the test equipment failure because it began to draw excessive current from the power supplies.

One module exhibited two failures during the first month of testing. Another module lasted 20 days of testing before experiencing its first failure and then degraded rapidly. The ninth module experienced three failures after only a few days of test and then stabilized until the flood, after which it degraded rapidly.

Only one module out of the nine had to be removed from the tester due to drawing excessive current, however. Eight finished the test period of 57 days.

In general, the frequency of failures could be correlated with deterioration of the magnesium-lithium frame (causing the RTV seal to peel off the circuit board). The failure mechanisms seemed, therefore, to be a moisture leakage under the edge of the RTV seal rather than by means of the connectors. Detailed examination and disecting of the failed modules supported this conclusion.

Although it is believed that the connector sealing technique was proven by the evaluation test, further testing is planned (under IBM funding, since the AES-EPO study period has concluded) with better sealed modules to eliminate module failures and provide further proof of the connector sealing capabilities. These tests will be reported to NASA-MSC.

4.0 CONCLUSIONS AND RECOMMENDATIONS

The two major objectives of the study have been achieved. A TMR computer system derived by reconfiguring the Saturn V guidance computer and the Apollo backup data adapter was shown to be a feasible solution to the time critical reliability problem. Also, a detailed investigation of inflight maintenance (including module and channel switching) as a means of solving the long term reliability problem was generally successful in all areas affecting maintenance activities including error detection, failure isolation, and module replacement in the high humidity, zero gravity AES environment.

4.1 Mission Requirements

The mission reliability requirements of 0.9994 for the 90-day mission period and 0.999999 for the critical phases of the mission were shown by the study to be feasible in a computer system provided only that one is willing to pay the cost of triple modular redundancy, built-in test and switching circuitry, and spares. Automatic error detection and fault isolation can be instrumented to relieve the inflight crew of the nearly impossible task of diagnosing error symptoms in complex digital systems. Automatic self-repair of the computer system was found in the study to be feasible. Also, manual repair (module replacement) was proved by laboratory test to be feasible in the adverse AES environment.

4.2 TMR Organization

The apportioned computer-data adapter reliability was specified to be 0.999999 for the critical phases of the 90-day earth polar orbit mission. The most critical phase of the mission for which the reliability estimates were made was the boost phase with an effective time period of 10.8 hours (obtained by multiplying real boost time by estimated environmental stress factors). The estimated reliability of the reconfigured computer system in its basic TMR mode of operation somewhat exceeded the requirement. In the TMR/Simplex mode of operation, where a module containing a component failure may be operated simplex while the rest of the modules operate TMR, an even greater reliability margin was realized with the reconfigured computer.

31

A conclusion of this study is that a TMR machine organization should be considered for any mission containing critical phases during which normal operation cannot be suspended to perform tests or to make repairs.

4.3 Inflight Maintenance

The apportioned computer-data adapter reliability was specified to be 0.9994 for the 90-day earth polar orbit mission. The estimated reliability of the reconfigured computer system in its basic TMR mode of operation without inflight maintenance was 0.9979. In the TMR/ Simplex mode the estimate was 0.9984, and for the Switchable Spare mode (in which the switched-out good module of the TMR/Simplex mode is made available as a built-in spare in case of a second failure in the same module) the estimate exceeded the mission requirement.

Although spare modules are not required to meet the mission reliability requirement if the Switchable Spare mode is instrumented, a redefinition of the critical phase is necessary if no spares are carried on the AES-EPO mission. Since re-entry (defined as a critical phase in the study) is the last phase of the mission, it will be initiated with a computer system which is not fully TMR. The accumulated failures over the 90 days have not been corrected by replacing failed modules with spares so that the reliability of entry cannot exceed the mission reliability. The entire mission, including re-entry, could be accomplished with a reliability exceeding 0.999, however.

The spares requirements for the TMR mode of operation (assuming that the TMR/Simplex or Switchable Spares modes are not instrumented) are listed in Table 9. The spares requirements for the TMR/ Simplex mode were not estimated but will be somewhat less. The spares requirements for all three modes will be identical to Table 9 if a 0.999999-reliability requirement is imposed on the re-entry phase.

Error detection and fault isolation studies were performed using the Saturn V System Simulator to determine the feasibility of this aspect of inflight maintenance. Automatic error detection by means of built-in test circuitry and without the need for special test programs was demonstrated in both the Saturn V and AES computer configurations with an efficiency of over 99 percent (over 99 percent of the simulated errors were detected). Automatic failure isolation by means of built-in test circuitry was found to be feasible to the same degree of efficiency. Error detection and diagnosis functions are therefore not required of the crew.

The repair studies included both manual and automatic techniques. Manual repair was implemented conceptually by providing the crew with an error display board with an error light indicating each replaceable module. Automatic and semiautomatic repair concepts included various switching instrumentations, usually automatic with manual override capabilities. If installation constraints permit, a TMR computer system could be instrumented with a wired-in fourth (spare) channel and fully automatic error detection, failure isolation, and functional replacement of the failed module with a spare from the fourth channel.

Sealing studies including laboratory test proved the feasibility of designing modularized equipment to operate and be maintained in a high humidity, zero gravity environment. The conventional unit sealing techniques requiring overpressurization, relief valves, and purging were abandoned in favor of sealing the individual replaceable modules and providing protection for the exposed connectors. A gasket-silicone gel technique for protecting the connectors proved highly satisfactory in laboratory tests.

4.4 General

The module and channel switching studies required in the statement of work led into several interesting potential capabilities for TMR organizations. Although a thorough examination of these potential capabilities was beyond the scope of the study, sufficient effort was expended to determine that feasibility depended only upon the development of error detection and switching circuits with specific characteristics, and an appreciable amount of effort was therefore expended in the area of detection and switching.

As mentioned in the previous section, a self-repairing TMR computer system can be realized by means of wired-in spares and circuitry which will automatically detect errors, isolate the failures to specific channels within the failed modules, and switch in the spare in place of the failed element. These required detection, diagnostic, and switching functions can be supplied by the switchable voter developed during the study and described in Section 5 of this report.

TMR machine organization possesses inherent capabilities for multimode operation which have not been realized in practice. A TMR/Simplex mode (in which one or more modules of the machine may be operated simplex while the remaining modules operate TMR) was shown in the study to provide appreciable increase in mission

and critical phase reliabilities over the conventional TMR mode. A Switchable Spare mode (in which a failure can be tolerated in each of those modules in the TMR/Simplex mode which have switched to simplex operation) was shown to provide an additional reliability increase over the TMR/Simplex mode.

If the voters are redesigned so that the three channels of the TMR organization can be functionally isolated rather than selectively turned off, a "multiprocessing" mode would be feasible in which each channel can operate as a separate computer. In orbital activities, for example, one channel could perform the data management function related to experiments, another channel could perform a similar function related to life support. and the third could perform navigation and vehicle control functions. With somewhat more complexity in the addressing scheme (allowing each channel access to the memories of the other two channels), the channels could operate independently on different phases of the same complex problem. Even further, on an extremely complex problem in three dimensions, each channel could handle the computations involving components along one of the three coordinate axes.

TMR machine organization seems to be especially applicable to those missions which contain critical phases requiring extremely high reliability for relatively short periods of time and noncritical phases which may be interrupted in case of failure but which require relatively large data handling capacity. The TMR organization provides the high reliability for the critical phases and the three independent channels provide the large data management capacity for the noncritical phases.